SECURITY IN ROUTING PROTOCOLS OF AD-HOC NETWORKS: A REVIEW

Isa Maleki[1], Ramin Habibpour[2], Majid Ahadi[3], Amin Kamalinia[4]
[1]Department of Computer Engineering, Dehdasht branch, Islamic Azad University, Dehdasht, Iran

[1]{maleki.misa@gmail.com, maleki@iaudehdasht.ac.ir}

[2,3,4] Department of Computer Engineering, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran

{ramin.habibpour[2], majid.ahadi.1988[3], amin.kamalinia[4]}@gmail.com

ABSTRACT

The Ad-Hoc networks include wireless hosts which can be mobile, too. Necessarily, it doesn't be used any prefabricated structure in these networks. It means that there is no substructure such as central station, router, switch and/or any other things which are used in network structure. There are only several wireless nodes which connect non-neighbour nodes using adjacent nodes. Security in Ad-Hoc networks is of high particular importance. As there are not only a lot of problems in wired networks but also security problems such as easy listening and change the information being transferred, the possibility of identity theft, lack of participation and/or destroying routing operations, inability to use encrypted key distribution infrastructures and so on are available problems. One of the main security problems is providing a secure routing protocol in these networks. In recent years, it has been done considerable effort to provide a secure routing protocol in these networks. So, we in this paper, will discuss about routing protocols which have remarkable effect on Ad-Hoc networks security to recognize security problems in routing Ad-Hoc networks using different kinds of routing protocols such as Flooding, DSR, AODV, ARAN, Ariadne, SAODV and SEAD and determine the best routing protocol in security of case protocol.

KEYWORDS

Ad-Hoc Networks, Security, Secure Routing Protocol

1. INTRODUCTION

Rapid development in wireless networks has considerable growth in recent years. Wireless networks [1, 2] include several nodes which communicate with each other on more than a wireless channel. Some of these wireless networks are Ad-Hoc, wireless sensor network [3], cellular networks [4] and satellite networks [5]. Ad-Hoc networks have various applications due to inability to use pre-fabricated infrastructure [1]. They are easy to launch and use but finally are removed [1, 6]. It can be noted to personal applications such as connection to PC computers, notebooks to each other, popular applications such as vehicles and taxis, military applications such as army and war ships connections and emergency applications such as relief and rescue operations [7]. As participated nodes in network are responsible to perform routing, the routing security represents more attention than the others. It means that covering security to transport data or intended pack in a route is a difficult task [8, 9].

Ad-hoc networks have been considered important in recent years and the users tend to use a secure environment to transport data. It is required to provide a secure routing protocol to transport data in Ad-Hoc networks [10]. Due to the especial features of Ad-Hoc networks, providing a secure protocol face with several security challenges. As it is said, Ad-Hoc networks consist of several wireless nodes which make relationship and communicate with each other [11]. In Ad-Hoc networks, the mobility of nodes can change the route between two nodes. This leads to the network differences from other wireless ones [12]. Due to the all available problems, Ad-Hoc networks have been used because of their easy implementation and independency from pre-fabricated structures in most cases [1].

One of the main issues which introduce in each type of network is to route and find optimal ones from source to target. Routing in wired and wireless networks involved infrastructures in which access points are constant is an important and difficult problem and require special solutions and strategies [13]. Solving these issues in Ad-Hoc networks in which the nodes aren't constant and always change is really difficult and needs more arrangements. As there is no constant topology in these networks and the nodes arrangements can be always changed [1, 14]. In Ad-Hoc networks, these are nodes which do the routing process but it is possible security problems occur in nodes routing process such as internal and external attacks. To remove these problems, the experts have been introduced secure routing protocols [7].

We organize the following paper as follow: in the section 2, it is discussed about Ad-Hoc networks and their general features; in the section 3, the security in routing Ad-Hoc networks are explained; in the section 4, the secure routing protocols to transport data are reviewed and explained in detail; in the section 5, routing protocols are discussed and finally in the section 6, conclusion and future works are provided.

2. AD-HOC NETWORKS

Ad-Hoc networks, a wireless local area network is. It is so called peer-to peer network. As it is said, no prefabricated infrastructure is used such as central stations, routers and so on but there are some nodes which connect non-neighbour nodes using adjacent nodes [1, 15]. In these networks, data is exchanged via wireless network card and mobile hardware such as pocket PC or cell phone which enters to the covered domain of this network and connects to the similar equipment's. They don't connect to the wired network context so they are called Independent Basic Service Set (IBSS) [16]. Figure 1 indicates the structure of Ad-Hoc network.

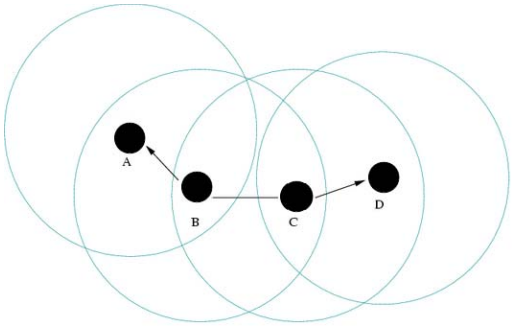

Figure 1. A Sample of ad-hoc networks structure

In Figure 1, the small circles indicate wireless nodes. Each big circle represents the useful range of a node. It means that any other node which located in this range can receive the delivered data of this node and identify them from environmental noises. To simplify the task, it is indicated

using a similar graph. The graph edges mean that two vertex of graph are in distances in which can receive each other messages. In fact, in graphic representation, the nodes which are located in useful range of a node can connect it by an edge.

2.1. The General Features of Ad-Hoc Networks

- **Mobility:** the nodes of Ad-Hoc networks can change their position rapidly. The nodes mobility is one of the features of Ad-Hoc networks. The rapid movement in places without infrastructure often indicates that users must look for a particular area or may be create a team or group which provides coordination and performs a particular activity. It can be created a particular accidental mobility, group mobility, movement among pre-determined routes and so on. The mobility type has an important effect on routing way as well as efficiency [17, 18].
- **Multi-Hoping:** multi-hoping is network which moves between source node and target several nodes. Ad-Hoc networks often provides hop to pass through barriers and save energy and also provides several small hops for operations under the cover of war field to decrease identification by enemy [19, 20].
- **Self-Organization:** Ad-Hoc networks must determine their configuration parameters which include addressing, routing, clustering, positioning, energy controlling and so on. Sometimes, particular nodes (e.g. mobile spinal nodes) can coordinate their movement and distribute in particular determined area dynamically to recognize cross sections [21, 22].
- **Energy Storing:** Ad-Hoc nodes often have battery power and limited energy and aren't capable of producing their own energy. Routing protocol designing which establishes proper energy is one of the main discussed issues [20].
- **Scalability:** Ad-Hoc networks can be increases to several thousand nodes in some applications (e.g. environmental sensors of big structures and buildings, battlefield elements and so on). For prefabricated wireless networks, scalability can be set up via providing hierarchical structure. Limited mobility of prefabricated networks can be easily set up related techniques of mobile IP. In contrast, increasing the number of nodes in Ad-Hoc networks will be a difficult task. So, mobility and connectivity to a larger scale is one of the main issues in Ad-Hoc networks [23].
- **Unmanned Autonomous Vehicle (UAV):** most well-known applications of Ad-Hoc networks require robotic and autonomous elements. All nodes of general networks are capable of independent networking. As the independent mobility is also added, it creates interesting circumstances to combine networking and mobility. For example, independent devices in flight or UAV can cooperate in maintaining a large group of Ad-Hoc network connections despite physical obstacles, disorder in channels distribution and enemy's interferences. Moreover, UAVs can help to increase efficiency using projectors antenna [24, 25].

3. SECURITY PROBLEMS OF ROUTING AD-HOC NETWORKS

In Ad-hoc networks not only there are security problems of routing data but also other problems such as recognizing abuse and influence [26]. In this paper, security problems of Ad-Hoc networks are reviewed to get familiar with these problems and secure routing protocols are also analyzed. Attacks against Ad-hoc networks can be classified from several viewpoints. In first viewpoint, classification can be as internal and external attacks [26]. Internal attacks are those which is performed by authorized nodes within the network and often difficult to prevent them. External attacks are those which are done by one or more attacks outside the network and often

security procedures are applied to prevent them. The other classification viewpoint depends on active or passive nature of attack. Passive or inactive attacks are those in which invader listens to the passing data but in active attacks invader changes the data in its favour. The next classification is invaded from network layers. It means that it can perform on physical layers, MAC, of network [26, 27]. Security problems of Ad-Hoc routing networks are divided in three main group of change, identity theft and falsifying. Of course, there are other types of attacks which resulted in prevention attacks of service such as refusing to participate in routing operation or disconnection in which it is available in all routing protocols and the only way to prevent it is to use hostile node [28]. In this paper, we begin to review attacks which located in subcategories of these three groups.

3.1. Wormhole Attack

One of the most important attacks of Ad-Hoc networks is wormhole attack. In this attack, two hostile nodes create a short connection in network topology. In noted attack the routing request from a node reaches to one of the hostile nodes. Here, this hostile node delivers the request through a private network for the second node. If these two nodes don't change the hop counter of route request, much of the route will be gone through this private network without increasing the amount of hop. So, it is possible that only two hops reach to the target rather ten of them. In this case, this route is surely selected as the shortest one. Another way to prevent wormhole attack is to use package preservative. The package preservative divided in two parts of time and place preservative. In time preservative, this technique based on precise synchronization of two source and target nodes and also using time seal in packages. So, by decreasing the amount of time seal as the package received, it is estimated the time interval in which the package was in the route. In this way, it is prevented from the number of hops in which time is more than logical time period. It means that due to the time interval in which the package is in the way and delivery rate of package in media, it can be estimated that how many hops can be passed through packages. So, it can be prevented from wormhole attack. In place preservative, this technique is based on place data. The target node can measure approximate distance of source node to itself due to the limited rate of nodes and so it prevents from unreasonable routes [7, 29].

3.2. The Attack of Routing Packages Field Change

A hostile node can lead to establish a wrong route by changing routing package fields. It can be done in different ways. For example, changing a route through changing a consecutive number is one of these ways. It can be explained as when a routing protocol uses a consecutive number in RREQ (Route Request) to correct prefabricated route, it can change the route in its favor due to the bigger consecutive number of RREQ messages which are in priority (if a hostile node is available). Another attack sample is to prevent service through changing source route. It can be said that as a routing protocol puts found route in sent packages header, the hostile node can change the inside route of header to prevent it to reach the target [7, 23].

3.3. Identity Change Attack

One of the other attacks in Ad-Hoc networks is the possibility of identity theft. It is as a node puts IP or MAC address of another node in its output packages. So, a node can impersonate in to another one [30]. Figure 2, indicates a sample of this attack which resulted in creating a loop.

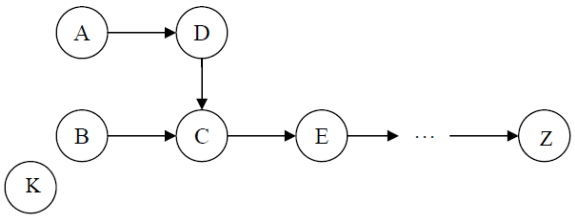

Figure 2. A Sample of identity theft in ad-hoc networks

In Figure 2, it is indicated a sample of identity theft in Ad-Hoc networks. It is assumed that represented routes for a route request will be through one of the routing protocols. Now, if node K moves toward node B and by using MAC, impersonate itself instead of node A, then, sends RREP (Route Reply) with zero hop count for B. at last, B changes the route toward A. in the next stage, node K changes its position and move toward C. By using MAC which belongs to B, it sends RREP with zero hop account for C. So, C changes its route toward B. In this stage, it is created a loop (A, D, C, B, A) [30].

One of the other classification methods of routing attacks is that it can be divided to two groups of routing conquered attacks and routing consumed attacks. In the first group of attacks, the hostile tries to send the packages as legal ones on the network to use them in the inefficient ways. In the second group, by sending packages, the hostile tries to consume and use network resources such as band width and/or node resources such as memory or computational power. From application layer viewpoint, both groups of these attacks are classified in service prevention attacks [28].

4. SECURE ROUTING PROTOCOLS TO TRANSPORT DATA

To create a secure route to transport data, a proper routing protocol in Ad-Hoc networks must create a route accurately and maintain it. It means that it doesn't let the hostile nodes prevent accurate building and maintaining of the route. In general, if, in a protocol, the points such as routing signals don't counterfeit, the manipulated signals can't be injected in to the network, routing messages don't change during transporting except protocol routines, routing loops don't create during aggressive activities, the shortest routes don't change by hostile nodes and so on are considered, it can be called a secure protocol [31]. To observe these points, we begin to review several protocols as far as possible.

4.1. Flooding

The simplest way to solve the routing problem in Ad-Hoc networks is to transport data through flooding. This method is as the data sender sends them to all neighbors' nodes. Each node which receives a data package also sends these data to its neighbors. To prevent sending a package by a node for more than once, it is used a consecutive number for each package. So, each receiver controls the package consecutive number and it is non-repetitive, sends it to all neighbors. By using this method, the data will certainly reach to the target. However, after reaching to the target, flooding process will be continued to end the receiving process [31, 32]. As it is clear, the main advantage of this method is the facility of implementation and then the assurance from reaching package to the target. But, the main problem of this method is that data packages are sometimes involves high volume and as it is explained, data may go through routes without necessity. For example, a node is proposed to send data to the neighbour node. Now, if Flooding method is used,

this package will issue in the all network. However, if we know about nodes' neighbors, we can decrease data transportation a lot. The increasing rate of network load causes that Flooding method doesn't be used to transport data. But, this method has been widely used in exchanging controlling signals due to the small size of these signals. The controlling packages are those used to get the route and send the data [32, 33].

4.2. DSR (Dynamic Source Routing)

In this protocol, the source node produces a package called RREQ in which it is determined source and target node. It sends these packages through flooding [34]. By receiving a RREQ package of each node, if it doesn't know about target route, then, it add its name to the package list and broadcast it. So, as the package reach to the target, a package includes data of route nodes and its arrangements will be available for the target node. The target node creates RREP and returns it back via available list in RREQ package header. The middle nodes know the target and do it according to the available list. So, the package traverses the route inversely to reach the source node. Although, it is a good method and certainly applicable but increases the network load and uses high band width which resulted in transporting large headers in the network. Increasing rate of header volumes resulted in increasing distance between source and target nodes. This volume increase is due to the name of network middle elements name in the package header. Then, data sender can put the target route in the sent data header to inform middle nodes through this route that to whom they send the package. When a node can't deliver data package to the next one, it produces a package called RERR (Route Error) and returns it back to the route. So, RERR receiving nodes acknowledges about these two nodes disconnection and routing operation will be started again [34, 35 and 36].

4.3. AODV (Advanced On-demand Distance Vector)

In contrast to DSR protocol, this protocol doesn't put the route in the package header. But, each node controls it while receiving PREQ according to tables it had before. If the route has the final node it its table, RREP will be sent. Otherwise, it broadcasts RREQ message. Certainly, RREPs can be returned back to RREQ. It is used consecutive number in RREQ messages that a middle node gets inform whether the route is a new one. So, if the number of RREQ consecutive is smaller than route consecutive number, RREP message will be sent by middle node [36, 37].

4.4. ARAN (Authenticated Routing for Ad-Hoc Networks)

It is based on encryption with general key and also using certificate. To provide routing security, ARAN protocol uses encrypted certificates [30]. These certificates have been used as a part of single hop 802.11 networks. ARAN protocol includes a process of issuing introductory certificate which follows by a route sampling process and guarantees the end-to-end authenticity. This protocol seems simple in compared to the others. Finding route in ARAN is done by a message of issued route finding from a source node which replies to the unicast state of target node as the routing messages are authenticated both along source to target route in each hop and inverse route from target to source. ARAN protocol is required to use T secure certificate issuing server in which its general key have been known for all authenticated nodes. The keys are primarily built and exchanged through the connection between T and each node. Prior to entering Ad-hoc network, each node must request a certificate from T. After that each node authenticates its authenticity for T securely, it only receives a certificate. The methods necessary to authenticate secure authenticity to certificate issuing server is handled by developers [30, 31]. For example, node A receives a certificate from T as equation (1).

$$T \to A : cert_A = [IP_A, K_{A^+}, t, e]K_{T^-} \quad (1)$$

Due to the equation (1), the variables of this certificate indicate that IP_A related to IP address of Node A, K_A related to general key of A, time seal t related to the certificate presented time and e indicates the expiring time. These variables are connected and sealed each other by T. All nodes must maintain new certificates using secure server. These certificates are used to authenticate the authenticity of node to the other nodes during routing messages exchange.

The goal of end-to-end authentication is that the source can determine whether reach to the desired target. In this process, the source relies on the target to select the destination route. For example, source node A begins to look for secure route to target Z by issuing route discovery package for its neighbors. It has several advantages such as it prevents from spoofing attacks which may be change the route or create a loop [31]. As the authenticated route is established, the source could reach to the desired target. This will prevent attacks in which routes hostile nodes provide modeling with identity theft and replaying message Z [31].

ARAN protocol is an on-demand one [30]. The nodes keep the tracking data of active routes. As there is no performed transportation on a route, it will simply become inactive in routes tables. Receiving data from an inactive route causes that the nodes create an error message which returns back to the source, inversely. The nodes also use error messages to report broken links in active routes due to the nodes movements. All error messages must be sealed. To reach the built time of error messages for active and accurate links is difficult. However, due to the sealed messages, the hostile nodes couldn't create error messages for other nodes. There is an undeniable state created by sealed error message and provides the possibility that the node recognizes as the source of each sent error message. It must be avoided the node which send a lot of error message whether valid or null [38, 39].

Unpredicted behavior can originate from a hostile node. But, it can also be associated with the wrong operation of neighbor nodes. ARAN reply for these two states isn't different and confronts against any unpredicted behavior in a same way. The unpredicted behavior includes using invalid certificates, inaccurate sealed messages and inaccurate using of route error messages. ARAN reply to unpredicted behavior is to anticipate a local decision and details are handled by implementation [38, 39].

In some environments which have determined security criterion, the required mechanism must be fully trusted. Due to low desired header in wireless networks and weak security standards which found in managed open environments, it can be provided an immediate expiring service which supported by using limited time certificates. When a certificate is proposed to expire, the trusted server of T certificate issuing sends a message to announce expiration for Ad-Hoc group. Equation (2) indicates this message.

$$T \to brdcast : [revoke, cert_r]K_{T^-} \quad (2)$$

Due to equation (2), each node receives this message and then sends it to the neighbors. Expiring announcements must be saved till the certificate expires normally. The neighbors of certificate that its certification is being expired must modify their routing to prevent unsecure transportation through that node. In this method, there is a possibility of failing. In some cases, unsecured node that its certification is being expired can be the only communication way of two parts in Ad-Hoc

networks. In this case, unsecured node may not send its certificate expiring announcement which resulted in network separation. As far as this unsecured node is the only way of communication between these two nodes, this state will remain constant [39, 40].
In general, ARAN protocol problems is due to non-resistance against wormhole attack. Another problem of this protocol is that it uses asymmetric encryption. So, it uses high energy and consequently had a lot of limitations in Ad-hoc networks [40].

4.5. Ariadne

In contrast with Ariadne protocol, ARAN protocol uses symmetric encryption. To authenticate the messages' accuracy, it is used Message Authentication Code. To do so, the code is structured by Hash function on received Hash message and the ID of sender node. So, each receiver can be sure about the authenticity of received message. In Ariadne protocol, each node which receives RREQ will authenticate itself as well as message by enclosing message authentication code. In this code, it is used the individual own ID and also the Hash of previous message in Hash function [29, 41].

It is secured under particular circumstances against wormhole attack. But the main problem is the need to exchange key between network nodes to do encryption before the protocol begins to perform [41].

4.6. SAODV (Secure AODV)

As it is clear from its name, it is provided to create more security in AODV [42]. In this protocol, it is used Hash functions as it is shown in equation (3).

$$h_{n-1} = H(h_n) \tag{3}$$

In equation (3), H is the function of Hash and h is the related to the hop. In this protocol, it is used hop count to measure the number of hops in which the packages go through. If the hop count becomes more than the amount of Max Count, the package will be ignored. To prevent the changes of hop count amount and make sure about the accuracy of its amount, it is used the noted Hash functions. Due to the equation (3), each node can be sure about its authenticity by receiving a message and controlling equation (3) on it. Number n also indicates the maximum hop that a package can go through [42, 43].

4.7. SEAD (Secure Efficient Ad-Hoc Distance Vector Routing)

In SEAD protocol, a routing table is available in each node in which there is a list of all possible targets in network. In each table, it is saved the address of targets, the nearest known distance which called metric and neighbour nodes which can be achieved to that target by next hop. These metrics are usually written in tables based on the number of hop [7, 44]. To update routing tables, each node sometimes sends a route request message to all its neighbors to be capable of putting new routes in its table. The first security development of SEAD is that it adds consecutive number to each routing table elements. These consecutive numbers prevent from creating loops which may be resulted in updating out of time routes. This protocol uses a one-way hashed series to provide security rather asymmetric encryption functions [7, 29]. To create one-way hashed series, each node selects a X number as $X \in \{0,1\}^{\rho}$ randomly (ρ is the number of output bits of hashed function) and makes the series of $h_0 = h_1,...,h_n$ as equation (4).

$$h_0 = X, h_i = H(h_{i-1}) \tag{4}$$

Each node of subsequent element of hashed Series which is sealed can be used in updating process. So, it is assumed a low threshold limit for consecutive numbers and metrics. So, any other node can create and issue new route with higher consecutive number or lower metric in the network. This causes to prevent disorder in updating routes in the network. In fact, SEAD prevents hostiles who change the issued data while route updating. If the hostile changes the amount of consecutive number and /or metric of a package, it creates problems for route updating. Replay attack is also considered important in SEAD. By receiving a route updating package and due to the amount of available hashed in it, the address of target node, package consecutive number, the previous receiving hashed, and the proper number of hash in new amount, each node cam confirmation the receiving package. To confirmation the accurate receiving of source nod, the proposed method is to use message authenticity code. This method is proposed to create a key between each two nodes [44].

5. DISCUSSION

Nowadays, due to data theft, data changes, time and cost consuming, a secure environment to transport data becomes one of the essential needs of human beings. To route data or files which is transported among nodes, the experts was always looking for a secure route to transport data secure and without any problem. To do so, routing protocols are created which remove security problems as far as possible. So, we propose to review routing protocols such as Flooding, DSR, AODV, ARAN, Ariadne, SAODV and SEAD to solve security problems. Table 1 shows the comparison between the routing protocols.

Table 1. Comparison of routing protocols

Parameters	**Protocols**						
	Flooding	**DSR**	**AODV**	**ARAN**	**Ariadne**	**SAODV**	**SEAD**
Wormhole Attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scalability Level	Not Suitable for Large Networks	Not Suitable for Large Networks	Not Suitable for Large Networks	Low	Low	Low	Low
Message Authentication Codes Used for Security	No	No	No	Yes	Yes	Yes	Yes
Routing Scheme	On demand	On demand	On demand	On demand	On demand	On demand	Table driven
Routing Overhead	Low	Low	Low	High	High	High	High
Path Accumulation	High	Low	Medium	High	High	Low	Low
Packet Dropping/ Delaying	High	Low	Low	Low	Low	Low	Very Low
Security Vulnerabilities	High	Low	Low	Low	Low	Very Low	Low

In Flooding protocol, it is perceived that there will be no more repeated packages in network which resulted in less traffic. Flooding protocol is easily implemented which resulted in easy receiving of package to the target. It plays also important role in transporting controlling signals due to their small volume. In DSR protocol, transporting packages is done by Flooding protocol in which there was routing request. In fact, it performs its transportation process via combination with Flooding protocol, so, it can be said that it performs better than flooding. In DSR, the nodes will determine the lack of connection between two nodes. AODV protocol is designed to control packages considering its tables. It also can support broadcast, unicast and multicast without any other protocol. ARAN protocol is designed to perform several main tasks such as issuing secured and trusted certificate to justify the authenticity of node than the other ones which are used during routing messages exchange. It also prevents from attacks which propose to change the route or creates a loop. In this protocol, the hostile nodes can't simulate routes via identity theft. In ARAN protocol, if it is occurred an error during routing, the nodes would be informed by error report message. It is also designed to encounter any unanticipated behavior from a hostile node. As it can be seen, dislike some protocols (such as ARAN) which use symmetric encryption as one of the best methods, Ariadne protocol is consistent against hole worm attacks. SAODV is same as AODV protocol but SAODV emphasizes more on routing security. In SEAD protocol, SAODV easily justifies the authenticity of nodes and can prevent Replay Attack as far as possible.

6. CONCLUSIONS AND FUTURE WORKS

As it is discussed, a secure route to transport data or information files in Ad-Hoc networks without any problem is the main need of users. So, several protocols are created in this feature to meet the security needs. Moreover, in this paper, we try to discuss about security problems in routing data to reveal the problems. Due to these problems, the main security issues are discussed and reviewed and perceive that there is strategies to solve for each protocols. The future works will be targeted to solve the problems by protocol combination in order to transport data with more security.

REFERENCES

[1] M.G. Zapata, N. Asokan, "*Securing Ad hoc Routing Protocols*", Proceedings of the ACM Workshop on Wireless Security (WiSe), pp. 1-10, September 2002.

[2] F. Xue, P.R. Kumar. "*Scaling Laws for Ad Hoc Wireless Networks: An Information Theoretic Approach*", Foundations and Trends in Networking. Vol. 13, No. 2, pp. 16-47, 2006.

[3] A. Sharifkhani, N.C. Beaulieu, "*A mobile-sink-based packet transmission scheduling algorithm for dense wireless sensor networks*", IEEE Transactions Vehicular Technology, Vol. 58, No. 5, pp.2509-2518, 2009.

[4] B. M. Epstein, M. Schwartz, "*Predictive QoS-based admission control for multiclass traffic in cellular wireless networks*", IEEE Journal on Selected Areas in Communications, Vol. 18, No. 3, pp. 523-534, March 2000.

[5] F. Yu, V.C. M. Leung, "*Mobility-Based Predictive Call Admission Control and Bandwidth Reservation in Wireless Cellular Networks*", Proceedings of IEEE INFOCOM'01 20th Annual Joint Conference of the IEEE Computer and Communications Societies, Alaska, USA, 2001.

[6] Y. Zhang, W. Lee, "*Intrusion Detection in Wireless Ad-Hoc Networks*", in The Sixth Annual ACM/IEEE Conference on Mobile Computing and Networking, Boston, MA, USA, pp. 275-283, Aug 2000.

[7] Y.C. Hu, A. Perrig, "*A Survey of Secure Wireless Ad Hoc Routing*", IEEE Security and Privacy 2004, Editorial Calendar, Vol. 2, No. 3, pp. 94-105, May/June 2004.

[8] L. Zhou, Z. J. Haas, "*Securing Ad Hoc Networks*", IEEE Network Magazine, Vol. 13, No. 6, pp. 24-30, Nov 1999.

[9] A. Iwata, C. Chiang, G. Pei, M. Gerla, T.W. Chen, "*Scalable routing strategies for ad hoc wireless networks*", IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, pp. 1369-1379, August 1999.

[10] Y. Peiyan, L. Layuan, "*Performance Evaluation and Simulations of Routing Protocols in Ad Hoc Networks*", Proceedings of International Workshop on Broadband Wireless, ACM, Alghero, Italy, 20 September 2006.

[11] S.A.K. Al-Omari, P. Sumari, "*An over view of Mobile Ad Hoc Networks for Existing Protocols and Applications*", International Journal on Applications of Graph Theory in Wireless Ad-hoc Networks and Sensor Networks (Graph-Hoc), Vol. 2, March 2010.

[12] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, E.B. Royer, "*A Secure Routing Protocol for Ad Hoc Networks*", Proceedings of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[13] S. Carter, A. Yasinsac, "*Secure Position Aided Ad Hoc Routing*", Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02), 3-4 Nov 2002.

[14] B. Strulo, J. Farr, A. Smith, "*Securing mobile ad hoc networks a motivational approach*", BTTechnology Journal, Vol. 21, No. 3, pp. 81-90, 2003.

[15] M. Masdari, S. Jabbehdari, M. Ahmadi, S. M. Hashemi, J. Bagherzadeh, A. Khadem-Zadeh, "*A survey and taxonomy of distributed certificate authorities in mobile ad hoc networks*", EURASIP Journal on Wireless Communications and Networking, 2011.

[16] S. Sharma, A. Dhamija, V. Rawal, "*Current issues with Ad-hoc network & proposed solutions*", International Journal of Applied Engineering Research, Vol.7, No.11, 2012.

[17] T.N. Vidanagama, H. Nakazato, "*Mobility in a description based clustered ad hoc network*", IEEE, GLOBECOM Workshops (GC Wkshps), Tokyo, Japan, pp. 148-152, 2010.

[18] V. Vetriselvi, R. Parthasarathi, "*Trace Based Mobility Model for Ad Hoc Networks*", Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, White Plains, NY, 8-10 Oct 2007.

[19] L. Jiandong , Z.J. Haas, M. Sheng, "*Capacity evaluation of multi-channel multi-hop ad hoc networks*", IEEE International Conference on Personal Wireless Communications, pp. 211-214, 15-17 Dec. 2002.

[20] S. Vijay, S.C. Sharma, "*EEN: An Energy Efficient Multi-Hop Ad Hoc Wireless Networks*", First International Conference on Emerging Trends in Engineering and Technology, Nagpur, Maharashtra, pp. 145-150, 2008.

[21] A. Akl, T. Gayraud, P. Berthou, "*An investigation of self- organization in ad-hoc networks*", IEEE International Conference on Networking, Sensing and Control (ICNSC), Delft, pp. 1-6, 11-13 April 2011.

[22] N. Asokan, P. Ginzboorg, "*Key-Agreement in Ad-hoc Networks*," In The Fourth Nordic Workshop on Secure Computer Systems, Vol. 23, pp. 1627-1637, 1999.

[23] L.H. Huang, T.H Lai, "*On the Scalability of IEEE 802.11 Ad Hoc Networks*", Proceedings of the 3rd ACM international Symposium on Mobile Ad-hoc Networking & Computing, EPFL Lausanne, Switzerland, pp. 173-182, 2002.

[24] S. Chaumette, R. Laplace, C. Mazel, A. Godin, "*Secure cooperative ad hoc applications within UAV fleets position*", IEEE, Military Communications Conference (MILCOM), pp. 1-7, Boston, MA, 2009.

[25] R.C. Palat, A. Annamalau, J.H. Reed, " Cooperative relaying for ad-hoc ground networks using swarm UAVs", IEEE, Military Communications Conference (MILCOM), pp. 1588 - 1594, Atlantic City, NJ, 2005.

[26] E.M. Royer, C.K. Toh, "*A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks*", IEEE Personal Communications, Vol. 6, No. 2, pp. 46-55, April 1999.

[27] S. Yi, P. Naldurg , R. Kravets, "*A Security-Aware Routing Protocol for Wireless Ad Hoc Networks*", in Proceedings of ACM Symposium on Mobile Ad-Hoc Networking & Computing (MOBIHOC), pp. 286-292, 2002.

[28] Y.C. Hu, A. Perring, D.B. Johnson, "*Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols*," Proceedings of the 2003 ACM workshop on Wireless security,San Diego, USA, pp. 30-40, 2003.

[29] S. Basagni, M. Conti, S. Giordano, I. Stojmenovic, "*Mobile Ad-hoc Networking*", IEEE press, John Wiley and Sons publication, pp. 329-354, 2004.

[30] K. Sanzgiri, B. Dahilly, B.N. Levine, C. Shields, E.M. B. Royer, "*A Secure Routing Protocol for Ad Hoc Networks*", Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), pp. 1-10, 2002.

[31] S. Prakash, J.P. Saini, S.C. Gupta, "*Methodologies and Applications of Wireless Mobile Ad-hoc Networks Routing Protocols*", International Journal of Applied Information Systems, Vol. 1, No. 6, pp. 5-15, February 2012.

[32] A. Boukerche, "*Performance comparison and analysis of ad hoc routing algorithms*", in Proc. of IEEE International Conference on Performance, Computing, and Communications, pp. 171-178, 2001.

[33] G. Pei, M. Gerla, T.W. Chen, "*Fisheye state routing: a routing scheme for ad hoc wireless networks*," in Proc. of IEEE International Conference on Communications, pp. 70-74, 2000.

[34] D. Johnson, D. Maltz, Y. Hu, "*The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*", IETF Internet-Draft, 2011.

[35] N.S.M. Usop, A. Abdullah, "*Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment*", IJCSNS International Journal of Computer Science and Network Security, Vol. 9, No.7, pp.261-268, July 2009.

[36] A. Akbari, M. Soruri, A. Khosrozadeh, "*A New AODV Routing Protocol in Mobile Adhoc Networks*", World Applied Sciences Journal, Vol. 19, No. 4, pp. 478-485, 2012.

[37] D. Benetti, M. Merro, L.Viganò, "*Model Checking Ad Hoc Network Routing Protocols: ARAN vs. endairA*", IEEE 8th International Conference on Software Engineering and Formal Methods (SEFM), Pisa, pp. 191-202, Sep 2010.

[38] A. Mahmoud, A. Sameh, S. El-Kassas, "*Reputed authenticated routing for ad hoc networks protocol (reputed-ARAN)*", IEEE International Conference on Mobile Ad-hoc and Sensor Systems, Washington, DC, 2005.

[39] S. Mehla, B. Gupta, P.Nagrath, "*Analyzing security of Authenticated Routing Protocol (ARAN)*", International Journal on Computer Science and Engineering (IJCSE), Vol. 02, No. 03, pp. 664-668, 2010.

[40] Y.C. Hu, A. Perrig, D.B. Johnson, "*Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks*", in Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pp. 12-23, September 2002.

[41] F. Maan, Y. Abbas, N. Mazhar, "*Vulnerability assessment of AODV and SAODV routing protocols against network routing attacks and performance comparisons*", Wireless Advanced (WiAd), London, pp. 36-41, June 2011.

[42] B. Smith, S. Murthy, J.J. Garcia-Luna-Aceves, "*Securing Distance Vector Routing Protocols*", in Internet Society Symposium on Network and Distributed System Security, the 7th International Workshop on Security Protocols, San Diego, CA, USA, pp. 85-92, Feb 1997.

[43] Y.C. Hu, D.B. Johnson, A. Perrig, "*Secure efficient distance vector routing in mobile wireless ad hoc networks*", in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications(WMCSA'02) , pp. 3-13, June 2002.

[44] C.H. Lin, W.S. Lai, Y.L. Huang, M.C. Chou, "*I-SEAD: A Secure Routing Protocol for Mobile Ad Hoc Networks*", International Conference on Multimedia and Ubiquitous Engineering, pp. 102-107, April 2008.

Authors

Isa Maleki is a Lecturer and Member of The Research Committee of The Department of Computer Engineering, Dehdasht Branch, Islamic Azad University, Dehdasht, Iran. He Also Has Research Collaboration with Dehdasht Universities Research Association Ngo. He is a Member of Review Board in Several National Conferences. His Interested Research Areas Are in the Machine Learning, Data Mining, Optimization, Artificial Intelligence and Wireless Networks.

Ramin Habibpour is a M.Sc. student in Computer Engineering Department, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran. His interested research areas are Network Security, Routing Algorithm of Networks and Wireless Sensor Networks.

Majid Ahadi is a M.Sc. student in Computer Engineering Department, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran. His interested research areas are Network Security, Routing Algorithm of Networks and Wireless Sensor Networks.

Amin Kamalinia is a M.Sc. student in Computer Engineering Department, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran. His interested research areas are Network Security, Routing Algorithm of Networks and Wireless Sensor Networks.